



EUROPEAN PATENT APPLICATION

Application number: 89102139.6

Int. Cl. 4: G07B 17/02

Date of filing: 08.02.89

Priority: 08.02.88 US 153391

Date of publication of application:  
16.08.89 Bulletin 89/33

Designated Contracting States:  
DE

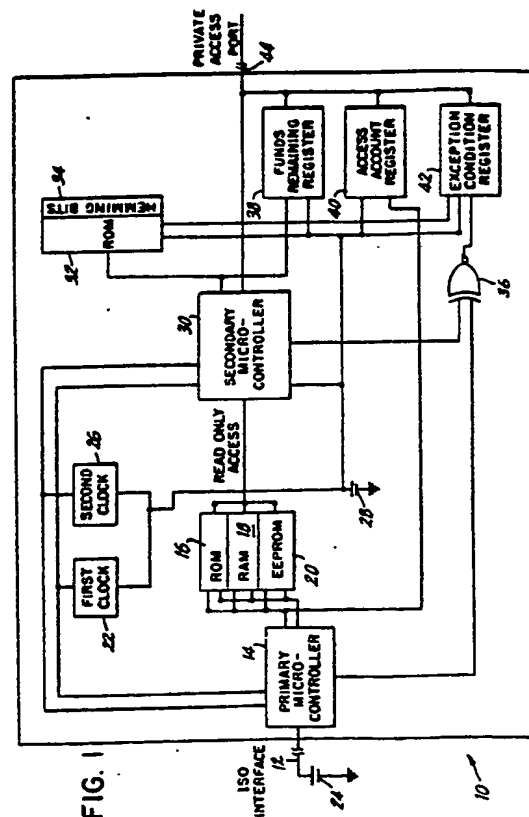
Applicant: PITNEY BOWES, INC.  
World Headquarters One Elmcroft  
Stamford Connecticut 06926-0700(US)

Inventor: Winslow Jackson E.  
26 Watch Hill Road  
Monroe CT 06468(US)

Representative: Ritter und Edler von Fischern,  
Bernhard, Dipl.-Ing. et al  
HOFFMANN - EITLE & PARTNER  
Arabellastrasse 4  
D-8000 München 81(DE)

54 Fault tolerant smart card.

57 A fault tolerant smart card (10) is provided having primary functional units including a standard ISO interface (12), a first microcontroller (14), a clock (22, 26), and main memory (16, 18, 20). Secondary functional units including a secondary microcontroller (30), secondary memory (32) with bit checking capability (34) and an alternate battery power source (28) are also provided. A microcontroller error detector (36) is connected to both microcontrollers (14, 30). Should a discrepancy between microcontrollers (14, 30) occur known test patterns are run on the second microcontroller (30) to determine which microcontroller is faulty. A private access port (44) provides alternate access to information stored in the fault tolerant smart card (10). Registers for funds remaining (38), error condition (42) and access account (40) are also provided.



## FAULT TOLERANT SMART CARD

### TECHNICAL FIELD

The present invention relates to a fault tolerant smart card and, more specifically, to a fault tolerant smart card which may find particular application in the postage meter industry.

### BACKGROUND AND OBJECTS OF THE INVENTION

Integrated circuit or so-called "intelligent" or "smart" cards which include a microprocessor and memory are commercially available and are useful in many applications. Of increasing importance is the ability of smart cards to securely transport monetary funds, including transportation of postal funds or information relating to postage funds. See, for example, U.S. application serial no. (attorney docket C-343) entitled "Postal Charge Accounting System" wherein departmental postage meter use information is stored in smart card memory, and U.S. application serial no. (attorney docket C-341) entitled "Postage Meter Value Card System" wherein postage meter funds are transferred from a value card center to a postage meter for recharging the postage meter vault.

Given the increasing importance of information stored in smart card memory, the adverse effects of a malfunctioning smart card can be quite costly. Therefore, it would be highly desirable to provide a smart card having increased reliability. It would also be highly desirable to provide a smart card which may be accessed by service personnel even were a card malfunction to occur. In this manner, monetary funds stored in the card would not be "lost" due to card malfunction.

Therefore, it is an object of the present invention to provide an improved smart card.

It is another object of the invention to provide a fault tolerant smart card.

It is yet another object of the invention to provide access to information retained in memory of a smart card which suffers a malfunction.

These and other highly desirable objects and advantages are obtained in a convenient yet secure fault tolerant smart card.

Objects and advantages of the invention are set forth in part herein and in part will be obvious herefrom, or may be learned by practice with the invention, the same being realized and attained by means of the instrumentalities and combinations pointed out in the appended claims.

### SUMMARY OF THE INVENTION

In accordance with the present invention a fault tolerant smart card is provided having primary functional units including a standard ISO interface, a primary microcontroller, main memory including ROM, RAM and EEPROM, a clock generator and a power source. In addition to its normal smart card functions the primary microcontroller addresses an access account register and a microcontroller fault detector which, in turn, addresses an exception register. Secondary smart card functional units are provided including a secondary microcontroller, secondary memory which may include ROM and associated check bits, a funds remaining shadow register, the access account register, the microcontroller fault detector, and the exception condition register. A private access port is also provided. All of the secondary units requiring power support are connected to an alternate battery power source. The secondary microcontroller is connected to the primary and secondary clock units, the microcontroller fault detector and the funds remaining register. The secondary microcontroller addresses the secondary memory and has read-only access to the main memory.

In normal operation the primary and secondary microcontrollers operate synchronously and execute in parallel identical instructions from the same memory store, but with the secondary microcontroller having read-only access to the main memory.

Should the microcontroller fault detector sense a fault in either of the main or secondary microcontrollers, as evidenced by an inconsistency between microcontroller signals, the exception register will be written into. When this occurs the primary microcontroller will be maintained in a frozen state and the secondary microcontroller will be released from the main memory to address the secondary memory and run known test patterns. Should a fault occur during the test the secondary microcontroller is assumed to be faulty and the main microcontroller will be permitted to continue processing. Of course, the user might be notified that card service and/or replacement is required.

On the other hand, if no error occurs during the test then the main microcontroller is assumed to be faulty, the card remains inoperable, and the user is notified by an appropriate flag that a card fault condition exists.

Advantageously, the private access port permits service personnel to directly access the secondary microcontroller, the funds remaining register,

ter, the access account register and the exception condition register. Service personnel might also make use of the secondary microcontroller, such as to access in read-only fashion the main memory. In the preferred embodiment including check bits the check bits would detect and circumvent any single bit failure in the secondary memory.

Thus, it will readily be appreciated that the fault tolerant smart card according to the present invention advantageously provides a smart card capable of detecting and circumventing a single bit or single path failure. Notwithstanding such a failure, the fault tolerant smart card remarkably provides "back-door" access through a private access port to important information held in the smart card. Advantageously, the person acquiring access through the private access port is able to determine the amount of any funds remaining in the card and access other important information in the card main memory. As a further advantage of the present invention the primary functional units communicate via the standard ISO interface in a traditional manner. Therefore, the fault tolerant smart card in accordance with the invention may be used in conjunction with existing, unmodified equipment. By way of example only, the fault tolerant smart card according to the present invention may find particular application in the systems disclosed in the aforementioned patent applications.

It will be understood that the foregoing general description as well as the following detailed description are exemplary and explanatory of the invention but are not restrictive thereof.

#### BRIEF DESCRIPTION OF THE DRAWING

The accompanying drawing, referred to herein and constituting a part hereof, illustrates in schematic block diagram form the preferred embodiment of a fault tolerant smart card in accordance with the present invention.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Referring now to the drawing, labelled as Figure 1, there is shown a schematic block diagram illustration of the fault tolerant smart card 10 in accordance with the invention. As shown, smart card 10 includes a set of primary functional units including a standard ISO type interface 12, a microcontroller unit 14, addressable read-only memory (ROM) 16, random access memory (RAM) 18, electronically erasable programmable read-only

memory (EEPROM) 20, primary and secondary clock generators 22, 26, respectively, and a primary power source 24. The preferred General Electric smart card referred to in the aforementioned patent applications derives power through the ISO interface, as shown, but an external primary power supply is not critical to the present invention. The foregoing elements, interconnected as shown, comprise the primary functional units for carrying out normal operation of the smart card.

In addition, secondary functional units are provided for fault tolerant card support. The secondary units include a second clock generator 26 connected to an alternate battery power source 28 and to both microcontrollers 14, 30. The secondary microcontroller is connected to secondary memory 32, a microcontroller fault detector 36, and a funds remaining shadow register 38. Preferably, check bits 34 are provided in association with secondary memory 32 to monitor single bit failures within the secondary memory. As shown, the secondary microcontroller is connected in an addressable manner to ROM 32 and to funds remaining register 38. Secondary microcontroller 30 is also connected to a private access port 44 and has read-only access to main memory 20. Secondary microcontroller 30 is supported by primary power source 24 and alternate battery source 28. An access account register 40 and an exception condition register 42 addressed by the microcontroller fault detector are also provided. Each of funds remaining register 38, access account register 40, and exception condition register 42 are also connected to private access port 44 and are supported by battery source 28. Secondary memory 32 is also supported by battery source 28 and is connected to exception condition register 42. Access account register 40 is addressed by primary microcontroller 14 and is written into after each card use to maintain a history trace of the identity of the user, the memory address accessed, and the information stored at that address.

So constructed, the present smart card circuit provides detection and circumvention of single bit and single path smart card faults. During normal operation both microcontrollers 14, 30 work in a synchronous mode of operation to execute in parallel identical instructions from the same memory store. After each transaction secondary microcontroller 30 updates funds remaining register 38 to provide a running summary of the funds that remain stored in the card.

Should a discrepancy occur between the main and secondary microcontrollers the microcontroller fault detector, here shown as exclusive "OR" gate 36, would trigger a high output signal, thereby writing into exception condition register 42. If the exception register 42 is written into, program in-

formation in secondary memory 32 will direct secondary microcontroller 30 to release main memory 16, 18, 20 and run known test patterns stored in secondary memory 32. During this time main microcontroller 14 remains in a frozen state. Should a fault occur during the test, secondary processor 30 is assumed to be faulty and main processor 14 is permitted to continue processing. However, if no faults are found during the known test pattern, the main processor 14 is assumed to be faulty and the user is notified of a fault condition. Thereafter, information access is limited to proprietary interface 44, which is preferably available only to service personnel. Notwithstanding a main processor fault, service personnel may access each of the funds remaining register 38, access account register 40, and exception register 42 through private access port 44. Main memory 16, 18, 20 might also be accessed through port 44 if secondary microcontroller 30 remains viable. In this regard, secondary memory 32 is preferably provided with associated check bits, sometimes referred to as "Hemming Bits", to circumvent any bit failures within secondary memory 32.

Thus, the fault tolerant smart card according to the invention substantially eliminates the risk that funds and/or accounting information stored in the card will be lost due to card failure. Indeed, should a card failure occur, service personnel may simply access the remaining funds amount and other information held in main memory and transfer this information to a new smart card or other recording medium. In this manner the customer is assured that monetary funds and information will not be compromised due to a smart card malfunction. As will be readily appreciated, this capability will avoid the deleterious effects to customer relations that might otherwise result from such card failures.

Thus, the fault tolerant smart card according to the present invention advantageously detects smart card failures and, notwithstanding such a failure, permits private access to important information stored in the faulty card.

To the extent not already indicated, it will be understood that the invention in its broader aspects is not limited to the specific embodiments herein shown and described but departures may be made therefrom within the scope of the accompanying claims, without departing from the principles of the invention and without sacrificing its chief advantages.

## Claims

1. A fault tolerant smart card (10) comprising:  
a standard input-output interface (12);  
clock means (22, 26) for providing a time reference

during smart card operations;

main memory means (16, 18, 20) for storing program and data information;

first microcontroller means (14) connected to said interface (12), said clock means (22, 26) and said main memory means (16, 18, 20) for performing normal smart card functions;

secondary microcontroller means (30) connected to said first microcontroller means (14), said clock means (22, 26), said main memory means (16, 18, 20) and to secondary memory means (32) for performing normal smart card functions in synchronization with said first microcontroller means (14);

microcontroller error detection means (36) connected to said first microcontroller means (14) and said secondary microcontroller means (30) for detecting a failure of either of said first or secondary microcontrollers (14, 30); and

primary power supply means (24) connected to said first microcontroller means (14).

2. The fault tolerant smart card (10) according to claim 1 wherein said secondary microcontroller means (30) has read-only access to said main memory means (16, 18, 20).

3. The fault tolerant smart card (10) according to claim 1 wherein said clock means (22, 26) further comprise a primary clock (22) and a secondary clock (26), said secondary clock (26) being connected to a secondary battery power means (28).

4. The fault tolerant smart card (10) according to claim 1 further comprising an access account register (40) connected to and addressed by said first microcontroller means (14) for providing a history trace of user identity and memory locations addressed by prior users.

5. The fault tolerant smart card (10) according to claim 1 wherein said secondary memory (32) further comprises read-only memory (32) including programming for running one or more known test patterns on said second microcontroller (30).

6. The fault tolerant smart card (10) according to claim 5 wherein said secondary memory programming is activated by said microcontroller error detection means (36) upon detection of a failure in either of said first or second microcontroller means (14, 30).

7. The fault tolerant smart card (10) according to claim 6 wherein, upon indication of a microcontroller failure by said microcontroller error detection means (36), said first microcontroller (14) is maintained in a frozen state while said secondary microcontroller (30) runs said known test patterns.

8. The fault tolerant smart card (10) according to claim 7 wherein, should an error occur in said known test patterns, said secondary microcontroller (30) is assumed to be faulty and said first microcontroller (14) is permitted to continue processing.

9. The fault tolerant smart card (10) according to claim 7 wherein, should no error occur in said known test patterns, said first microcontroller (14) is assumed to be faulty and card failure is indicated to the user.

10. The fault tolerant smart card (10) according to claim 9 further comprising private access port means (44) connected to said second microcontroller means (30) for permitting service access to the fault tolerant smart card (10).

11. The fault tolerant smart card (10) according to claim 10 further comprising a funds remaining register (38) connected to said second microcontroller (30) and further connected to and accessible through said private access port means (44) for indicating a remaining amount of funds stored in the fault tolerant smart card (10).

12. The fault tolerant smart card (10) according to claim 10 further comprising access account means (40) connected to said first microcontroller means (14) and connected to and accessible through said private access port means (44) for providing a history trace of user identity memory locations addressed by prior users.

13. The fault tolerant smart card (10) according to claim 11 wherein said secondary microcontroller (30), said secondary memory (32), and said funds remaining register (38) are connected to a secondary battery power source (28).

14. The fault tolerant smart card (10) according to claim 12 wherein said secondary microcontroller (30), said secondary memory (32) and said access account means (40) are connected to a secondary battery power source (28).

15. The fault tolerant smart card (10) according to claim 10 further comprising checking bit means (34) associated with said secondary memory (32) for detecting and circumventing single bit or single path failures within said secondary memory (32).

16. The fault tolerant smart card (10) according to claim 1 wherein said microcontroller error detection means (36) further comprise an exclusive "OR" gate (36) furnished with the output signal of each of said first and second microcontrollers (14, 30), said exclusive "OR" gate (36) being triggered to produce an error signal should a discrepancy occur between said microcontroller output signals.

17. A fault tolerant smart card (10) comprising:  
a standard input-output interface (12);  
clock means (22, 26) for providing a timer reference during smart card operations;  
main memory means (16, 18, 20) for storing program and data information;  
first microcontroller means (14) connected to said interface (12), said clock means (22, 26) and said main memory means (16, 18, 20) for performing normal smart card functions;  
secondary microcontroller means (30) connected to

said first microcontroller means (14), said clock means (22, 26), said main memory means (16, 18, 20) and to secondary memory means (32), said secondary microcontroller means (30) performing normal smart card functions in synchronization with said first microcontroller means (14),  
microcontroller error detection means (36) connected to said first and secondary microcontroller means (14, 30) for detecting a discrepancy between said first and secondary microcontroller means (14, 30); and private access port means (44) connected to said secondary microcontroller (30) for providing private access to the fault tolerant smart card (10).

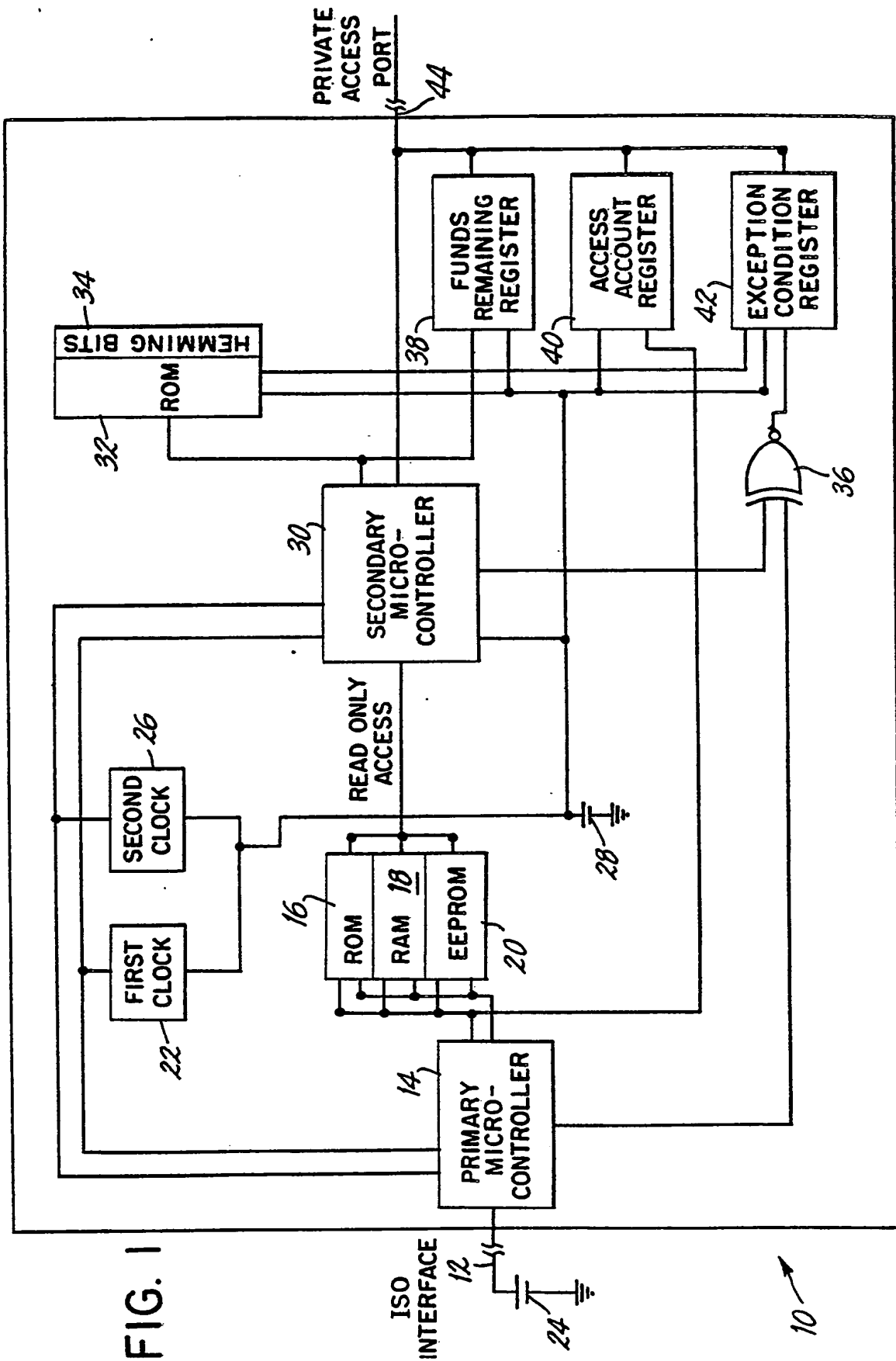
18. The fault tolerant smart card (10) according to claim 17 wherein, upon detection of an error by said microcontroller error detection means (36), said first microcontroller (14) is maintained in a frozen state and said secondary microcontroller (30) is released from said main memory means (16, 18, 20) to run known test patterns under the direction of said secondary memory means (32).

19. The fault tolerant smart card (10) according to claim 18 wherein, should an error occur during said known test patterns, said secondary microcontroller (30) will be assumed faulty and said first microcontroller (14) will be permitted to continue processing.

20. The fault tolerant smart card (10) according to claim 18 wherein, should no error occur during said known test patterns, said first microcontroller (14) is assumed faulty and a faulty card signal is transmitted to the user.

21. The fault tolerant smart card (10) according to claim 20 wherein said private access port (44) permits access to information contained in said main memory means (16, 18, 20).

22. The fault tolerant smart card (10) according to claim 21 further comprising a funds remaining register (38) connected to said secondary microcontroller (30) and said private access port means (44) for storing information relating to available funds remaining within the fault tolerant smart card (10).





Europäisches Patentamt  
European Patent Office  
Office européen des brevets



Publication number:

**0 328 062 A3**

12

## EUROPEAN PATENT APPLICATION

21 Application number: 89102139.6

51 Int. Cl.<sup>5</sup>: G07B 17/02

22 Date of filing: 08.02.89

30 Priority: 08.02.88 US 153391

43 Date of publication of application:  
16.08.89 Bulletin 89/33

84 Designated Contracting States:  
DE

88 Date of deferred publication of the search report:  
18.09.91 Bulletin 91/38

71 Applicant: **PITNEY BOWES, INC.**  
World Headquarters One Elmcroft  
Stamford Connecticut 06926-0700(US)

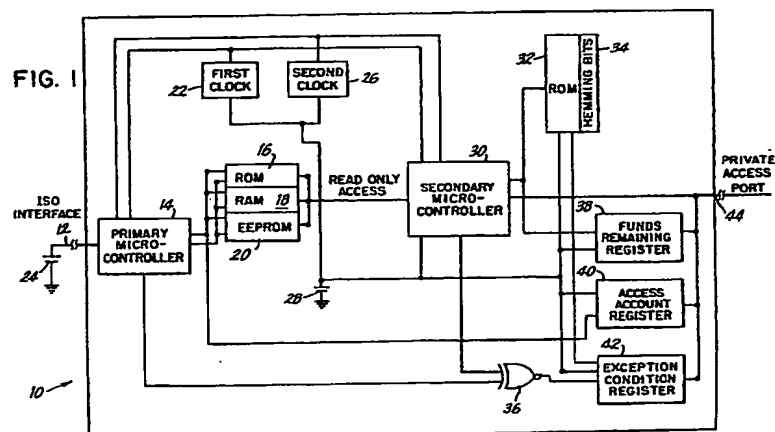
72 Inventor: **Winslow Jackson E.**  
26 Watch Hill Road  
Monroe CT 06468(US)

74 Representative: **Ritter und Edler von Fischern,**  
Bernhard, Dipl.-Ing. et al  
**HOFFMANN - EITLE & PARTNER**  
Arabellastrasse 4  
W-8000 München 81(DE)

54 Fault tolerant smart card.

57 A fault tolerant smart card (10) is provided having primary functional units including a standard ISO interface (12), a first microcontroller (14), a clock (22, 26), and main memory (16, 18, 20). Secondary functional units including a secondary microcontroller (30), secondary memory (32) with bit checking capability (34) and an alternate battery power source (28) are also provided. A microcontroller error detector (36) is connected to both microcontrollers (14, 30).

Should a discrepancy between microcontrollers (14, 30) occur known test patterns are run on the second microcontroller (30) to determine which microcontroller is faulty. A private access port (44) provides alternate access to information stored in the fault tolerant smart card (10). Registers for funds remaining (38), error condition (42) and access account (40) are also provided.



EP 0 328 062 A3



European  
Patent Office

## EUROPEAN SEARCH REPORT

Application Number

EP 89 10 2139

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
A	WO-A-8 603 040 (INTELLICARD INTERNATIONAL) * page 19, line 3 - page 21, line 11; figures * - - -	1,3,10,17, 21	G 07 B 17/02 G 06 K 19/06 G 06 F 11/00
A	GB-A-2 185 443 (PITNEY BOWES) * page 7, lines 30 - 97; figures * - - -	1,4,5, 11-14,17, 22	G 06 F 11/16 G 06 F 11/26
A	US-A-4 353 064 (STAMM) * column 2, line 45 - column 3, line 24; figures * - - -	1,3,13,14, 16,17	
A	EP-A-0 147 599 (I.B.M. CORPORATION) * page 2, line 28 - page 3, line 27; figures * - - -	1,6,7,17, 18	
A	EP-A-0 217 281 (CASIO COMPUTER) * page 2, column 1, line 16 - column 2, line 41; figures * - - - - -	1	
			TECHNICAL FIELDS SEARCHED (Int. Cl.5)
			G 07 B G 06 K G 06 F G 07 F
The present search report has been drawn up for all claims			
Place of search		Date of completion of search	Examiner
The Hague		23 July 91	RAKOTONDRAJAONA C.N.
<div>CATEGORY OF CITED DOCUMENTS</div> <div>X : particularly relevant if taken alone</div> <div>Y : particularly relevant if combined with another document of the same category</div> <div>A : technological background</div> <div>O : non-written disclosure</div> <div>P : intermediate document</div> <div>T : theory or principle underlying the invention</div> <div>E : earlier patent document, but published on, or after the filing date</div> <div>D : document cited in the application</div> <div>L : document cited for other reasons</div> <div>&amp; : member of the same patent family, corresponding document</div>			